IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Peter Szor		
Assignee:	Symantec Corporation		
Title:	KERNEL MODE OVERFLOW ATTACK PREVENTION SYSTEM AND METHOD		
Serial No.:	10/781,207	Filed:	February 17, 2004
Examiner:	Unknown	Group Art Unit:	2182
Docket No.:	SYMC1048		

Monterey, CA
May 25, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner.

U.S. PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	NAME
1)	5,696,822	12/09/97	Nachenberg
2)	5,822,517	10/13/98	Dotan
3)	6,301,699	10/09/01	Hollander et al.
4)	6,357,008	03/12/02	Nachenberg

OTHER DOCUMENTS

1)	Szor, P., U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
2)	Szor, P., U.S. Patent Application Serial No. 10/371,945, filed February 21, 2003, entitled "SAFE MEMORY SCANNING".

3)	Szor, P., U.S. Patent Application Serial No. 10/464,091, filed June 17, 2003, entitled "SEND BLOCKING SYSTEM AND METHOD".
4)	Szor, P., U.S. Patent Application Serial No. 10/611,472, filed June 30, 2003, entitled "SIGNATURE EXTRACTION SYSTEM AND METHOD".
5)	Szor, P., U.S. Patent Application Serial No. 10/681,623, filed October 7, 2003, entitled "UNMAPPED CODE BLOCKING SYSTEM AND METHOD".
6)	Szor, P., *"Attacks on WIN32"*, Virus Bulletin Conference, October 1998, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 57-84.
7)	Szor, P., *"Memory Scanning Under Windows NT"*, Virus Bulletin Conference, September 1999, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-22.
8)	Szor, P., *"Attacks on WIN32-Part II"*, Virus Bulletin Conference, September 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
9)	Chien, E. and Szor, P., *"Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses"*, Virus Bulletin Conference, September 2002, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
10)	Buysse, J., *"Virtual Memory: Windows NT® Implementation"*, pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://people.msoe.edu/~barnicks/courses/cs384/papers19992000/buyssej-Term.pdf.
11)	Dabak, P., Borate, M. and Phadke, S., *"Hooking Windows NT System Services"*, pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:www.windowslibrary.com/Content/356/06/2.html.
12)	*"How Entercept Protects: System Call Interception"*, pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/kernekmode.asp. No author provided.
13)	*"How Entercept Protects: System Call Interception"*, pg. 1 [online]. Retrieved April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/interception.asp. No author provided.
14)	Kath, R., *"The Virtual-Memory Manager in Windows NT"*, pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/dngenlib/html/msdn_ntvmm.asp?frame=true.
15)	Szor, P. and Kaspersky, E., *"The Evolution of 32-Bit Windows Viruses"*, Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.winnetmag.com/Articles/Print.cfm?ArticleID=8773.
16)	Szor, P., *"The New 32-bit Medusa"*, Virus Bulletin, December 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.

17)	Szor, P., *"Shelling Out"*, Virus Bulletin, February 1997, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.
18)	McCorkendale, B. and Szor, P., *"Code Red Buffer Overflow"*, Virus Bulleting, September 2001, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.
19)	Nachenberg, C., *"A New Technique for Detecting Polymorphic Computer Viruses"*, University of California, Los Angeles, 1995.
20)	*"INFO: CreateFileMapping() SEC_* Flags"*, pp.1-2 [online]. Retrieved on September 24, 2003. Retrieved from the internet: URL:http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1. No author provided.
21)	*"CreateFileMapping"*, pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/fileio/base/createfilemapping.asp?frame=true. No author provided.

A PTO form 1449 listing these documents is enclosed.

Citation of the above documents shall not be construed as:

1. an admission that the documents are necessarily prior art with respect to the instant invention;

2. a representation that a search has been made, other than as described above; or

3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 25, 2004.

Attorney for Applicant(s)

May 25, 2004
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
(831) 655-0880

Sheet 1 of 7

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1048	Serial No. 10/781,207
	Applicant(s) Peter Szor	
	Filing Date February 17, 2004	Group 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,696,822	12/09/97	Nachenberg	380	4	
	AB	5,822,517	10/13/98	Dotan	395	186	
	AC	6,301,699	10/09/01	Hollander et al.	717	4	
	AD	6,357,008	03/12/02	Nachenberg	713	200	
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

	AR	Szor, P., U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
	AS	Szor, P., U.S. Patent Application Serial No. 10/371,945, filed February 21, 2003, entitled "SAFE MEMORY SCANNING".
	AT	Szor, P., U.S. Patent Application Serial No. 10/464,091, filed June 17, 2003, entitled "SEND BLOCKING SYSTEM AND METHOD".

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449	**Atty Docket No.** SYMC1048	**Serial No.** 10/781,207
INFORMATION DISCLOSURE CITATION **IN AN APPLICATION**	**Applicant(s)** Peter Szor	
(Use several sheets if necessary)	**Filing Date** February 17, 2004	**Group** 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Szor, P., U.S. Patent Application Serial No. 10/611,472, filed June 30, 2003, entitled "SIGNATURE EXTRACTION SYSTEM AND METHOD".
	AS	Szor, P., U.S. Patent Application Serial No. 10/681,623, filed October 7, 2003, entitled "UNMAPPED CODE BLOCKING SYSTEM AND METHOD".
	AT	Szor, P., "*Attacks on WIN32*", Virus Bulletin Conference, October 1998, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 57-84.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 INFORMATION DISCLOSURE CITATION IN AN APPLICATION *(Use several sheets if necessary)*	Atty Docket No. SYMC1048	Serial No. 10/781,207
	Applicant(s) Peter Szor	
	Filing Date February 17, 2004	Group 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Szor, P., *"Memory Scanning Under Windows NT"*, Virus Bulletin Conference, September 1999, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-22.
	AS	Szor, P., *"Attacks on WIN32-Part II"*, Virus Bulletin Conference, September 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
	AT	Chien, E. and Szor, P., *"Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses"*, Virus Bulletin Conference, September 2002, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION** **IN AN APPLICATION** *(Use several sheets if necessary)*	**Atty Docket No.** SYMC1048	**Serial No.** 10/781,207
	Applicant(s) Peter Szor	
	Filing Date February 17, 2004	**Group** 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Buysse, J., *"Virtual Memory: Windows NT® Implementation"*, pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://people.msoe.edu/~barnicks/courses/cs384/papers19992000/buyssej-Term.pdf.
	AS	Dabak, P., Borate, M. and Phadke, S., *"Hooking Windows NT System Services"*, pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.windowsitlibrary.com/Content/356/06/2.html.
	AT	*"How Entercept Protects: System Call Interception"*, pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/kernekmode.asp. No author provided.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION** **IN AN APPLICATION** *(Use several sheets if necessary)*	**Atty Docket No.** SYMC1048	**Serial No.** 10/781,207
	Applicant(s) Peter Szor	
	Filing Date February 17, 2004	**Group** 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	*"How Entercept Protects: System Call Interception"*, pg. 1 [online]. Retrieved April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/interception.asp. No author provided.
	AS	Kath, R., *"The Virtual-Memory Manager in Windows NT"*, pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/dngenlib/html/msdn_ntvmm.asp?frame=true.
	AT	Szor, P. and Kaspersky, E., *"The Evolution of 32-Bit Windows Viruses"*, Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.winnetmag.com/Articles/Print.cfm?ArticleID=8773.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 **INFORMATION DISCLOSURE CITATION** **IN AN APPLICATION** *(Use several sheets if necessary)*	**Atty Docket No.** SYMC1048	**Serial No.** 10/781,207
	Applicant(s) Peter Szor	
	Filing Date February 17, 2004	**Group** 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Szor, P., "*The New 32-bit Medusa*", Virus Bulletin, December 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.
	AS	Szor, P., "*Shelling Out*", Virus Bulletin, February 1997, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.
	AT	McCorkendale, B. and Szor, P., "*Code Red Buffer Overflow*", Virus Bulletin, September 2001, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449	**Atty Docket No.** SYMC1048	**Serial No.** 10/781,207
INFORMATION DISCLOSURE CITATION **IN AN APPLICATION**	**Applicant(s)** Peter Szor	
(Use several sheets if necessary)	**Filing Date** February 17, 2004	**Group** 2182

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (*Including Author, Title, Date, Pertinent Pages, Etc.*)

	AR	Nachenberg, C., "*A New Technique for Detecting Polymorphic Computer Viruses*", University of California, Los Angeles, 1995.
	AS	"*INFO: CreateFileMapping() SEC_* Flags*", pp.1-2 [online]. Retrieved on September 24, 2003. Retrieved from the internet: URL:http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1. No author provided.
	AT	"*CreateFileMapping*", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/fileio/base/createfilemapping.asp?frame=true. No author provided.

Examiner	Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).